

Direzione

Gianvito Giannelli, Ugo Patroni Griffi, Antonio Felice Uricchio, Andrea Patroni Griffi

Comitato scientifico

Sabino Fortunato (**coordinatore**) - Lorenzo De Angelis - Pietro Masi - Cinzia Motti - Antonio Nuzzo - Luigi Filippo Paolucci - Salvatore Patti - Michele Sandulli - Gustavo Visentini

Redazione di Bari

Emma Sabatelli, Giuseppina Pellegrino, Eustachio Cardinale, Francesco Belviso, Rosella Calderazzi, Barbara Francone, Anna De Simone, Valentino Lenoci, Enrico Scoditti, Emma Chicco, Claudio D'Alonzo, Giuditta Lagonigro, Manuela Magistro, Francesco Salerno, Concetta Simone

Redazione di Foggia

Michele Bertani, Andrea Tucci, Giuseppe Di Sabato, Corrado Aquilino, Pierluigi Pellegrino, Grazia Pennella, Annalisa Postiglione, Annamaria Dentamaro, Attilio Altieri, Giulia Lasalvia

Redazione di Lecce

Maria Cecilia Cardarelli, Alessandro Silvestrini, Giuseppe Positano, Andrea Sticchi Damiani

Redazione di Napoli

Andrea Patroni Griffi, Alfonso M. Cecere, Nicola De Luca, Carlo Iannello, Sergio Marotta, Francesco Sbordone, Pasquale Serrao d'Aquino

Redazione di Roma

Giustino Enzo Di Cecco, Paolo Valensise, Vincenzo Vitalone, Valeria Panzironi, Ermanno La Marca, Valentina Depau, Davide De Filippis

Redazione di Taranto

Daniela Caterino, Giuseppe Labanca, Cira Grippa, Gabriele Dell'Atti, Giuseppe Sanseverino, Pietro Genoviva, Francesco Sporta Caputi, Barbara Mele

Direzione

Piazza Luigi di Savoia n. 41/a

70100 – BARI - (Italy)

tel. (+39) 080 5246122 • fax (+39) 080 5247329

direzione.ibattellidelreno@uniba.it

Coordinatore della pubblicazione on-line: Giuseppe Sanseverino

Redazione: presso il Dipartimento Jonico in Sistemi Giuridici ed Economici del Mediterraneo:

Società, Ambiente, Culture - Sezione di Economia -

Via Lago Maggiore angolo Via Ancona

74121 - TARANTO - (Italy)

tel (+39) 099 7720616 • fax (+39) 099 7723011

redazione.ibattellidelreno@uniba.it

giuseppe.sanseverino@uniba.it

ISSN 2282-2461 I Battelli del Reno [on line]

I Battelli del Reno, rivista on line di diritto ed economia dell'impresa, è registrata presso il Tribunale di Bari (decreto n. 16/2012)

La rivista è licenziata con Creative Commons Attribuzione – Non commerciale – Non opere derivate 3.0 Italia (CC BY-NC-ND 3.0 IT)

Ignazio Tardia*

RESPONSABILITÀ PER ILLECITO TRATTAMENTO DEI DATI
NELL'IMPIEGO DI DRONI: PROFILI SOSTANZIALI E RIMEDIALI**

SOMMARIO: 1. Tecnologie emergenti e vulnerabilità giuridiche: droni, IA e *privacy* tra innovazione e riallocazione del rischio. – 2. Ciclo di vita del dato nei sistemi UAS+IA: progettazione, minimizzazione e sicurezza. – 3. La dimensione regolatoria multilivello tra GDPR, AI Act e disciplina UAS. – 4. Il modello di responsabilità per illecito trattamento *ex art. 82 GDPR*: *accountability*, colpa presunta e prova liberatoria. – 5. Persona e proporzionalità nella legittimità del volo-dato.

1. Tecnologie emergenti e vulnerabilità giuridiche: droni, IA e privacy tra innovazione e riallocazione del rischio. La migrazione dalla videosorveglianza tradizionale – stanziale, prevedibile, territorialmente confinata – a piattaforme dotate di sensoristica avanzata, mobili e pervasive, quali i sistemi aeromobili a pilotaggio remoto (*Unmanned Aircraft Systems-UAS*)¹, determina un salto qualitativo nella capacità di raccolta, correlazione e inferenze dai dati personali². Il drone non è (più) una mera “telecamera volante”: è un nodo cognitivo

*Professore associato di Diritto privato – Dipartimento di Giurisprudenza – Università degli Studi di Palermo

** *Sottoposto a referaggio*

¹ In generale, si veda la recente ricostruzione di R. BELLOTTI e L. TAFARO (a cura di), *Mezzi aerei a pilotaggio remoto: questioni teoriche e profili applicativi*, Napoli, 2021. Per B. FRANCHI, *L'evoluzione della normativa internazionale e UE relativa agli unmanned aircraft, detti anche «droni»: profili ricognitori*, in *Resp. civ. prev.*, 2018, p. 1790 ss., tali mezzi si stanno sempre più diffondendo nello scenario aeronautico internazionale per il risparmio di costi a parità di missione rispetto ad un aeromobile *manned*, per la possibilità di operare senza rischi per l'equipaggio in ambienti c.dd. 3D (*dirty, dull e dangerous*) e per la capacità di operare su vaste aree, per prolungati periodi di tempo, senza bisogno di rientrare alla base per consentire l'avvicendamento degli equipaggi. Peraltro, la pandemia da Covid-19 ha evidenziato le potenzialità di utilizzo dei droni anche in tema di sanità (consegna di materiale medico, comunicazione delle linee guida sul distanziamento sociale, sanificazione di edifici e strade, ecc.): cfr., sul punto, M. LAMON, *La rivoluzione aeronautica dei sistemi aerei a pilotaggio remoto e il loro esercizio nella lotta alla pandemia da Covid-19*, in *Dir. mar.*, 2021, p. 249 ss., e F. GASPARI, *La regolazione multilivello degli aeromobili a pilotaggio remoto e la disciplina speciale dell'ENAC nel contesto della pandemia da Covid-19*, in *Riv. dir. nav.*, 2020, p. 139 ss.

itinerante³, capace di acquisire in sincronia immagini ad alta risoluzione, flussi audio direzionali, telemetrie, metadati di geolocalizzazione, identificativi di rete, nonché caratteristiche comportamentali⁴ suscettibili di ricondurre a una persona fisica identificata o identificabile⁵. L'integrazione con moduli di intelligenza artificiale⁶ (*computer vision, pattern recognition, object tracking*) accresce l'intensità intrusiva del trattamento: l'analisi automatica dei flussi sensoriali abilita la profilazione, la re-identificazione e l'estrazione di correlazioni latenti che eccedono la mera registrazione dell'immagine. In questa metamorfosi, il rischio per la *privacy* non deriva soltanto dal "quanto" si raccoglie, ma dal "come" i dati sono

² Sul tema v., tra gli altri, A. DAVOLA, *L'acquisizione di dati da parte dei privati nelle operazioni con SAPR*, in E. PALMERINI, M.A. BIASIOTTI e G.F. AIELLO (a cura di), *Diritto dei droni. Regole, questioni e prassi*, Milano, 2018, p. 137 s.

³ Sulla costante espansione di tale settore, cfr. F. MORANDI, L. ANCIS, F. TONEATTO, C. SEVERONI e S. VERNIZZI, *Il panorama normativo in materia di mezzi aerei a pilotaggio remoto e lo stato della sua implementazione in Italia – I Parte*, in *Resp. civ. prev.*, 2022, p. 1087, nota 4.

⁴ E. DAMIANI, *L'utilizzo dei droni e le inerenti ricadute sul diritto della privacy e della responsabilità civile*, in *Dir. merc. tecn.*, 2021, p. 22 ss., che osserva come l'impiego degli aeromobili a pilotaggio remoto consenta «di raccogliere, produrre e sviluppare una grande quantità di dati di varia tipologia (immagini, dati biometrici, dati di spostamento, dati di comunicazione...) vista la loro maggiore libertà di movimento anche a bassa quota, grazie alle dimensioni ridotte, e la presenza di tecnologie avanzate in grado di sopperire alla mancanza di un pilota fisico a bordo»: sul piano sociologico viene in rilievo anche il c.d. «chilling effect» o «effetto dissuasivo», «derivante dall'aumento della sensazione di essere costantemente sottoposti a sorveglianza, con una possibile conseguente riduzione dell'esercizio di diritti e libertà civili».

⁵ Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero d'identificazione, dati relativi all'ubicazione, un identificativo *online* o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. Il riferimento è chiaramente al reg. (UE) n. 679/2016 (GDPR), su cui si vedano, senza alcuna pretesa di esaustività, V. CUFFARO, *Il diritto europeo sul trattamento dei dati personali*, in *Contr. impr.*, 2018, p. 1098 ss.; G. VISINTINI, *Dal diritto alla riservatezza alla protezione dei dati personali*, in *Dir. inf.*, 2019, p. 1 ss.; A. PISAPIA, *La tutela per il trattamento e la protezione dei dati personali*, Torino, 2018; A. MORACE PINELLI, *La circolazione dei dati personali tra tutela della persona, contratto e mercato*, in *Nuova giur. civ. comm.*, 2022, II, p. 1322 ss.

⁶ IA che è definita nell'art. 3, § 1, n. 1, AI Act, come «un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'*input* che riceve come generare *output* quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali». In tema di IA esiste già un'ampia letteratura: tra i più recenti, cfr. G. FINOCCHIARO, *Intelligenza artificiale. Quali regole?*, Bologna, 2024; N. CRISTIANINI, *Machina sapiens. L'algoritmo che ci ha rubato il segreto della conoscenza*, Bologna, 2023; L. D'AVACK, *Intelligenza artificiale e diritto: problematiche etiche e giuridiche*, in *Dir. fam. pers.*, 2023, p. 1710 ss.; G. SARTOR, *L'intelligenza artificiale e il diritto*, Torino, 2022. Sul recente regolamento europeo, noto come AI Act, si vedano T.M. UBERTAZZI, *GDPR, European strategy for data and Artificial Intelligence Act. A functional perspective*, in *Contr. impr./Eur.*, 2023, p. 429 ss.; A. PISAPIA, *Cosa possiamo aspettarci dalla regolamentazione europea in materia di intelligenza artificiale?*, in *Cib. dir.*, 2023, p. 3 ss.; G. BARONE, *Artificial intelligence Act: un primo sguardo al regolamento che verrà*, in *Cass. pen.*, 2024, p. 1047 ss.

rielaborati, arricchiti e dalle inferenze che se ne traggono, generando conoscenza ulteriore a partire da segnali apparentemente innocui (c.d. *mosaic effect*)⁷.

Tre sono, in particolare, i fattori moltiplicativi del rischio introdotti dai droni. Innanzitutto, la “mobilità” del sensore: diversamente dagli impianti fissi, l’UAS riposiziona la piattaforma di ripresa in tempo reale, attraversa spazi eterogenei (pubblici, aperti al pubblico, privati), sorvola punti di vista altrimenti inaccessibili e rende strutturalmente arduo ogni previo adempimento informativo e di acquisizione del consenso⁸. Ne discende la frequente necessità di fare leva su basi giuridiche alternative e di una ponderazione attenta dei diritti e delle libertà fondamentali, specie in presenza di minori e categorie vulnerabili⁹. In secondo luogo, la scala e persistenza delle operazioni: la combinazione di

⁷ La particolare invasività del trattamento dei dati derivante dall’uso dei droni rispetto ai tradizionali strumenti di videosorveglianza, che sono caratterizzati da “immobilità”, è stata ben evidenziata dall’Art. 29 *Working Party*, che ha elaborato una serie di raccomandazioni, destinate ai legislatori nazionali e agli operatori del settore, allo scopo di implementare la tutela del diritto alla riservatezza delle persone in relazione all’uso dei droni: i risultati di tali attività sono confluiti nel parere «Privacy and Data Protection Issues Relating to the Utilization of Drones», emanato il 16 giugno 2015, ove viene sottolineata l’impellente necessità di approntare cautele alla protezione dei dati personali adeguate alle specifiche caratteristiche tecnico-operative dei mezzi in questione. Tale gruppo di lavoro – creato ex art. 29 della Dir. 95/46/CE, quale organismo consultivo europeo indipendente in materia di protezione dei dati e *privacy* – ha operato sino al 25 maggio del 2018, data di entrata in vigore del GDPR, che – all’art. 68 ss. – prevede l’istituzione del Comitato europeo per la Protezione dei dati (*European Data Protection Board*, EDPB).

⁸ Infatti, l’art. 6, § 1, GDPR stabilisce le condizioni che rendono lecito il trattamento dei dati personali, tra cui, in primo luogo, il consenso espresso dall’interessato per una o più specifiche finalità. In argomento, v. I.A. CAGGIANO, *Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo. Analisi giuridica e studi comportamentali*, in *Osserv. dir. civ. comm.*, 2018, p. 95 ss.; L. GATT, R. MONTANARI e I.A. CAGGIANO, *Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull’effettività della tutela dei dati personali*, in *Pol. dir.*, 2017, p. 376 ss.; G. BASUNTI, *La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali*, in *Contr. impr.*, 2020, p. 860 ss. Con riferimento alla giurisprudenza, v. Cass., 25 maggio 2021, n. 14381, in *Dir. inf.*, 2021, p. 1005 ss., con nota di F. BRAVO, *Rating reputazionale e trasparenza dell’algoritmo. Il caso “Mevaluate”*, e in *Resp. civ. prev.*, 2022, p. 498 ss., con nota di F. CASTAGNA, *Trasparenza algoritmica e validità del consenso al trattamento dei dati personali*, ove si sottolinea che «il consenso è validamente prestato solo se espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato». Tuttavia, l’acquisizione preventiva del consenso si rivela particolarmente complessa nelle operazioni condotte tramite UAS: in contesti aperti al pubblico, ad esempio, risulta spesso impossibile ottenere il consenso preventivo di tutti i soggetti potenzialmente coinvolti, specie in situazioni dinamiche, quali l’arrivo di passanti successivo all’avvio delle operazioni di volo e di acquisizione dei dati (v. le osservazioni di L. CALIFANO, *Spunti problematici sul trattamento dei dati personali raccolti tramite droni*, in *Cultura giuridica e diritto vivente*, 7/2020, p. 1 ss.).

⁹ In alternativa – ai sensi dell’art. 6, § 1, lett. f, GDPR – l’utilizzo dei dati personali può trovare giustificazione nel legittimo interesse del titolare del trattamento o di terzi, purché tale interesse prevalga sui diritti degli individui ripresi durante l’operazione, con particolare riguardo ai minori, considerati meritevoli di una tutela rafforzata. Spetterà, quindi, al titolare del trattamento effettuare un attento bilanciamento tra le esigenze perseguite e la tutela della riservatezza degli interessati, assumendosi la piena responsabilità delle conseguenze pregiudizievoli che potrebbero derivare dal trattamento, sia in caso di reclami da parte degli interessati, sia nel contesto di controlli operati dall’Autorità garante per la protezione dei dati personali. Qualora l’operazione effettuata mediante utilizzo di UAS sia riconducibile alla necessità di eseguire un «compito di interesse pubblico o connesso all’esercizio di pubblici poteri» (art. 6, § 1, lett. e, GDPR) e vi sia una base

voli ripetuti, lo stazionamento prolungato e la facilità di dispiegamento rendono ordinaria e continuativa la raccolta su larga scala, con correlati problemi di limitazione della finalità e di minimizzazione¹⁰. Ancóra, l'autonomia decisionale abilitata dall'IA: la classificazione quasi in tempo reale di volti, targhe, comportamenti, oggetti e punti critici trasferisce all'algoritmo scelte che impattano direttamente sul perimetro del trattamento (quali dati catturare, conservare, segnalare), imponendo misure di trasparenza, tracciabilità e controllo umano effettivo lungo tutto il ciclo di vita del sistema¹¹.

Con riguardo all'oggetto, il trattamento in ambito UAS non si esaurisce nell'immagine: comprende metadati (*timestamp*, coordinate, quota, *heading*, velocità), identificativi di rete, *pattern* comportamentali (traffico, flussi pedonali, permanenza in determinate aree) e, nei casi più avanzati, dati biometrici ricavati o potenzialmente ricavabili (si pensi al *face embedding* come possibile dato particolare ove trattato per l'identificazione univoca). Questa stratificazione semantica aumenta la probabilità di re-identificazione, anche quando il singolo strato informativo appaia non direttamente identificante: è l'accoppiamento dei livelli, facilitato da IA, a riattivare l'identificabilità del soggetto.

2. *Ciclo di vita del dato nei sistemi UAS+IA: progettazione, minimizzazione e sicurezza.* Sul piano tecnico-organizzativo, la catena del valore del dato UAS presenta molteplici superfici d'attacco che si riflettono, simmetricamente, sull'adozione di misure tecniche e organizzative adeguate (*ex art. 32 GDPR*). Durante la captazione, le scelte di *frame rate*, la risoluzione, lo *zoom* e il *field of view* determinano l'intensità del trattamento; nella trasmissione, i canali radio UAS-GCS (*Ground Control Station*) possono esporre flussi in tempo reale e telemetrie a intercettazioni ove la cifratura sia assente o debole; nella memorizzazione, la protezione degli archivi *on-board* e *off-board* nelle sue declinazioni perimetrali (stazione di terra/MEC locale) e in *cloud* richiede "robusta" gestione delle chiavi, separazione dei ruoli e tracciatura dei *log*; nella rielaborazione, i processi di IA

giuridica – stabilita dal diritto dell'Unione o dalla legislazione nazionale – da cui si evinca la finalità del trattamento (art. 6, § 3, GDPR), quest'ultimo potrà essere legittimamente eseguito.

¹⁰ Ai sensi dell'art. 5 GDPR, i dati personali devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (cfr. S.G. BATTISTINI, L. MATARAZZO e L. ZANETTI, *Il principio di minimizzazione dei dati*, in *Dati personali: protezione, libera circolazione e governance*, 1. *Principi*, a cura di F. Bravo, Pisa, 2023, p. 231 ss.).

¹¹ A. CAVOUKIAN, *Privacy by Design: The Definitive Workshop*, in *Identity in Information Society*, 2010, p. 247 ss., afferma che la tecnologia rappresenta lo strumento più consono per rafforzare la tutela della *privacy* mediante il ricorso alla c.d. «tecnoregolamentazione» (cfr. L. MERLA, *Droni, privacy e tutela dei dati personali*, in *Inf. dir.*, 1/2016, p. 29 s.; S. FAILLACE, *La natura e la disciplina delle obbligazioni di cui all'art. 25 del GDPR espressione dei principi di privacy by design e di privacy by default*, in *Contr. impr.*, 2022, p. 1123 ss.).

devono rispettare la protezione dei dati fin dalla progettazione (art. 25 GDPR)¹², assicurando – tra l’altro – pseudonimizzazione¹³, minimizzazione *ex ante*, *face blurring*¹⁴ e *area masking* come impostazioni predefinite, non già come opzioni *post hoc*. Tali profili – inclusa la possibilità di distinguere categorie operative “open”, “specific”, “certified” e i *risk assessment* correlati – sono espressamente considerati dal reg. es. (UE) n. 947/2019¹⁵ e dal reg. ENAC UAS-IT del 4 gennaio 2021¹⁶, che richiamano l’osservanza del GDPR e del

¹² L. CALIFANO, *Spunti problematici sul trattamento dei dati personali raccolti tramite droni*, cit., p. 7, osserva come le misure di *privacy by design* e *by default* siano ormai una realtà anche nel settore degli aeromobili a pilotaggio remoto. Ad esempio, il meccanismo di *geofencing*, che rappresenta un’adeguata garanzia per evitare la raccolta di dati ultronei: l’aprioristica circoscrizione dell’area di osservazione, nonché la preimpostazione delle informazioni da non memorizzare, costituiscono misure di minimizzazione dei dati. Allo stesso modo avviene con la predefinizione di tempi certi di conservazione, di cancellazione o anonimizzazione automatica delle immagini al termine del trattamento, come anche con la cifratura dei dati, per impedire che accessi indebiti possano comprometterne la riservatezza, l’integrità e la disponibilità.

¹³ Con tale espressione si indica un procedimento che mira ad impedire l’identificazione di un individuo attraverso i suoi dati. Tuttavia, a differenza dell’anonimizzazione, essa è una misura di sicurezza, consistente in un trattamento dei dati personali che riduce la possibilità di identificazione, facendo in modo che «i dati personali non possano più essere attribuiti ad un interessato specifico senza l’utilizzo di informazioni aggiuntive» (art. 4, § 5, GDPR). In proposito, E. PELLECCIA, *Dati personali, anonimizzati, pseudonimizzati, de-identificati: combinazioni possibili di livelli molteplici di identificabilità nel GDPR*, in *Nuove leggi civ. comm.*, 2020, p. 367 ss.; C. FOGLIA, *Il dilemma (ancora aperto) dell’anonimizzazione e il ruolo della pseudonimizzazione nel GDPR*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali tra libertà e regole di mercato. Commentario al Regolamento UE n. 2016/679 e al novellato d. lgs. n. 196/2003*, Torino, 2019, p. 309 ss.; C. IRTI, *Dato personale, dato anonimo e crisi del modello normativo dell’identità*, in *Jus Civile*, 2020, p. 379 ss.

¹⁴ Tecnica utilizzata per oscurare o rendere irriconoscibili i volti presenti in immagini o video.

¹⁵ Tale regolamento supera il precedente impianto fondato sulla distinzione tra scopi ricreativi (c.dd. «operazioni non specializzate») e professionali (c.dd. «operazioni specializzate»), applicando il nuovo approccio «performance and risk-based» (su tale approccio, cfr. M. HUTTUNEN, *Drone operations in the Specific Category: A Unique Approach to Aviation Safety*, in *Aviation Space J.*, 2/2019, p. 2; B.I. SCOTT, *Open Skies for Unmanned Aircraft in Europe: An Outlier or a New Approach?*, in *Air Space L.*, 2021, p. 60). La classificazione delle operazioni non è più stabilita in base alla finalità, bensì in funzione del grado di rischio e delle caratteristiche tecniche dell’aeromobile, distinguendo tre categorie: «open», «specific» e «certified», cui corrispondono regimi giuridici diversi. Le operazioni UAS (*Unmanned Aircraft System*) si considerano «open», con una bassa soglia di rischio, quando sono effettuate con droni dotati di marcatura CE di peso non superiore ai 25 kg, in modalità VLOS (*Visual Line Of Sight*) e a un’altezza massima di 120 m dal punto più vicino alla superficie terrestre, con un impiego che non necessita di alcuna autorizzazione o dichiarazione da parte dell’operatore, salvo il caso in cui il volo debba avvenire in spazi aerei controllati; «specific», quando presentano requisiti di rischio superiori, diversi dalla precedente categoria e che non rientrano in quella successiva, per cui è richiesta l’autorizzazione operativa da parte dell’autorità aeronautica nazionale o la dichiarazione preventiva da parte dell’operatore UAS (ad esempio, operazioni BVLOS, *Beyond Visual Line of Sight*); «certified», quando sono connotate da un rischio tale da imporre la preventiva autorizzazione operativa da parte dell’autorità aeronautica, la certificazione dell’operatore, il possesso da parte del pilota remoto della specifica licenza prevista dal reg. del. (UE) n. 945/2019 e la registrazione dell’UAS.

¹⁶ Con cui l’ENAC s’è prontamente adeguata all’evoluzione della normativa tecnica internazionale e dell’Unione europea con l’obiettivo di completare il quadro giuridico nazionale per le parti demandate alla regolamentazione interna.

Codice Privacy (d.lgs. n. 196/2003), con particolare attenzione al principio di minimizzazione.

Sotto il profilo sistemico, l'impatto dei droni sulla sfera privata non coincide con la sola cattura dell'immagine: la disponibilità di *dataset* longitudinali (atti a descrivere spostamenti, abitudini, orari, frequentazioni) abilita inferenze predittive sul comportamento futuro, con possibili esiti discriminatori laddove queste si innestino su modelli di *risk scoring* o *anomaly detection*. In questo orizzonte, l'esigenza di *governance* si sposta a monte: l'ordinamento pretende che il titolare, prima ancora di "accendere i sensori", dimostri (e non solo dichiari) di aver realizzato un percorso di progettazione conforme: analisi del contesto e delle basi giuridiche, definizione delle finalità (specifiche, esplicite, legittime), DPIA ove il rischio sia elevato¹⁷, misure tecniche e organizzative commisurate alla probabilità e alla gravità del pregiudizio (artt. 24 e 32 GDPR). È la traduzione concreta del principio di *accountability*, vera "architettura della prevenzione" del GDPR¹⁸.

Questo quadro si riflette anche sul momento informativo. Quando l'assetto operativo renda impraticabile un'informativa individuale *just-in-time*, il titolare deve ricorrere a strategie multilivello: pubblicità preventiva delle operazioni sul sito istituzionale; segnaletica *in situ* nelle aree di sorvolo; avvisi informativi sulla piattaforma digitale dell'operatore; identificazione chiara del responsabile e dei diritti esercitabili (artt. 12-14 GDPR). L'esperienza del provvedimento del Garante¹⁹ su *Google Street View-Special Collects*

¹⁷ La valutazione di impatto (*Data Protection Impact Assessment*), di cui all'art. 35 GDPR, è richiesta per quei trattamenti che, per loro natura, ambito di applicazione, contesto o finalità, possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Indipendentemente, quindi, dalla categoria dell'operazione («aperta», «specificata» o «certificata»), i titolari del trattamento dovranno autonomamente e preventivamente valutare se l'attività da essi posta in essere comporti rischi significativi per i diritti fondamentali degli interessati: il reg. es. (UE) n. 947/2019 stabilisce che, per le operazioni rientranti nella categoria «specificata», l'operatore di UAS è tenuto, qualora richiesto dall'autorità nazionale competente, a effettuare una valutazione d'impatto sulla protezione dei dati personali. La DPIA è obbligatoria anche nel caso di attività di sorveglianza sistematica su larga scala di una zona accessibile al pubblico (art. 35, § 3, lett. c, GDPR). Secondo E. DAMIANI, *L'utilizzo dei droni e le inerenti ricadute sul diritto della privacy*, cit., spec. p. 30, dal rispetto del principio della *privacy by design*, che richiede approcci di tipo proattivo, discende la generale previsione di «una valutazione d'impatto per i produttori di droni "progettati e prodotti" ai fini di sorveglianza e per gli operatori che usano droni con apparecchi "audiovisivi" a bordo».

¹⁸ Sul tema, tra i tanti, cfr. G. FINOCCHIARO, *Il principio di accountability*, in R. CATERINA (a cura di), *GDPR tra novità e discontinuità*, in *Giur. it.*, 2019, p. 2778 ss.; A. MANTELERO, *Responsabilità e rischio nel Reg. Eu 679/2016*, in *Nuove leggi civ. comm.*, 2017, p. 144 ss.; F. BRAVO, *Il consenso e le altre condizioni di liceità del trattamento dei dati personali. Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, in *Le riforme del diritto italiano*, 2017, p. 101 ss.

¹⁹ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Provvedimento di parziale esonero dall'informativa nei confronti di Google Inc. in relazione al servizio Street View-Special Collects*, 4 dicembre 2014, in *garanteprivacy.it*. In tale circostanza, il Garante richiese di informare gli interessati circa la programmata acquisizione di immagini relative ai siti mediante pubblicazione della notizia sul sito *web* di Google, almeno tre giorni prima dell'inizio delle operazioni, nonché tramite le pagine *web* e, se esistenti, le *newsletter* o altre pubblicazioni informative degli enti, strutture, soggetti privati, fondazioni, etc., che utilizzano le attrezzature del programma o che comunque possiedono, gestiscono o soprintendono i siti ovvero hanno altrimenti la

nel 2014)²⁰ offre un paradigma di mitigazione tramite informazione diffusa e riconoscibilità del dispositivo (adesivi, cartelli, annunci pubblici), mutuabile – con i dovuti adattamenti – alle operazioni UAS. Laddove la sfocatura automatica dei volti (c.d. *face blurring*) sia tecnicamente praticabile, tale misura concorre a riportare il trattamento entro i binari della proporzionalità (art. 5, § 1, lett. c, GDPR) e della protezione per impostazione predefinita (art. 25, § 2, GDPR). Un’ulteriore componente di rischio emerge dalla sicurezza “inversa”: i droni non solo possono essere adoperati per *hacking* o interferenze verso dispositivi terzi (*smart home, IoT*)²¹, ma sono esposti a compromissioni (presa di controllo del collegamento radio tra il drone e la stazione di terra – c.d. *takeover* del *link* – e *GPS spoofing*, solo per citarne alcuni)²², con possibili effetti a catena su integrità e riservatezza dei dati trattati²³.

disponibilità del rilascio della necessaria autorizzazione all’effettuazione delle riprese. Nell’eventualità di siti o luoghi, pubblici o privati, recintati ovvero aperti al pubblico, venne chiesto altresì di segnalare l’attività con avvisi o cartelli affissi all’ingresso dei siti interessati.

²⁰ Esso si occupa di acquisire immagini a 360 gradi relative a luoghi di particolare interesse artistico, storico, archeologico e naturalistico, come parchi nazionali, siti archeologici, *ski resort*, spiagge, castelli e giardini. A differenza del tradizionale *Google Street View*, tali acquisizioni avvengono in aree che non consentono il passaggio agevole delle automobili e richiedono quindi l’uso di operatori dotati di speciali apparecchiature, o, a seconda della natura del luogo, di imbarcazioni o treni. Il programma interessa anche luoghi privati o accessibili al pubblico solo in determinati orari, ove le immagini vengono raccolte in momenti in cui l’accesso al pubblico è precluso. Nei casi di spazi aperti come parchi, spiagge e sentieri di montagna, *Google* cerca di effettuare le riprese in momenti di bassa affluenza.

²¹ Si vedano le osservazioni di F. ABDULLAYEVA e O. VALIKHANLI, *A survey on UAVs security issues: attack modeling, security aspects, countermeasures, open issues*, in *Control and Cybernetics*, 2023, p. 405 ss. Attacchi di tipo «man-in-the-middle» o di «jamming» consentono, infatti, di intercettare informazioni trasmesse tramite *Wi-Fi*, inclusi dati bancari, *password* o altre informazioni sensibili: a mo’ d’esempio, un’azienda di sicurezza con sede a Londra, chiamata *Sensepoint*, aveva sviluppato uno *spyware* denominato *Snoopy*, che poteva essere equipaggiato su un drone, capace di carpire dai dispositivi mobili dati personali, come *password* utente di *PayPal*, *Amazon*, numeri di carta di credito e informazioni sulla posizione delle persone nelle vicinanze. Nel caso di specie, il drone – semplicemente passando nelle vicinanze della vittima – manipolava il dispositivo mobile con cui l’individuo stava interagendo, disconnettendolo dal *Wi-Fi* e inducendolo a connettersi a un punto di accesso falsificato, apparentemente attendibile: in questa maniera, l’aggressore riusciva ad ottenere l’accesso ai dati memorizzati nel telefono della vittima (*BBC News*, *Data-stealing Snoopy drone unveiled at Black Hat*, 28 marzo 2014, in [bbc.com/news/technology-26762198](https://www.bbc.com/news/technology-26762198)).

²² Cfr. Y. MEKDAK, A. ARIS, L. BABUN, A. EL FERGOUGUI, M. CONTI, R. LAZZERETTI, A. SELCUK ULUAGAC, *A survey on security and privacy issues of UAVs*, in *Computer Networks*, 2023, pp. 1-25; F. GRANIERI, *Navigating the Skies: A cross-country exploration of drone policies in Europe, USA and China, unveiling privacy and cybersecurity challenges*, in *J.L. Market Innovation*, 2/2024, p. 156 ss., ove, peraltro, il sistema europeo viene comparato a quelli statunitense e cinese.

²³ L’esigenza di un’effettiva tutela della *privacy* diventa ancor più intensa quando si tratta di sistemi aeromobili a pilotaggio remoto guidati da tecnologie di intelligenza artificiale, specie a causa dell’ingente quantità di dati che queste tecnologie possono trattare grazie a sistemi di «big data analytics»: per un’analisi approfondita dell’argomento, cfr. L. ZHU, F.R. YU, Y. WANG, B. NING, T. TANG, *Big Data Analytics in Intelligent Transportation Systems: A Survey*, in *IEEE Transactions on Intelligent Transportation Systems*, 2019, p. 383 s.

3. *La dimensione regolatoria multilivello tra GDPR, AI Act e disciplina UAS.* La disciplina europea *risk-based* degli UAS (reg. n. 1139/2018 e reg. n. 947/2019) e la regolazione nazionale (ENAC UAS-IT), anche alla luce dell'AI Act (che può qualificare come *high-risk* i sistemi di IA impiegati a bordo o a supporto delle operazioni, qualora ne ricorrano i presupposti, e introduce requisiti relativi alla qualità dei dati, alla documentazione, alla tracciabilità e alla supervisione umana²⁴), mirano a una convergenza tra *safety* e *security*: la protezione del dato non è un *add-on*, ma un requisito essenziale di progettazione dell'aeromobile e della sua architettura digitale (di bordo e di terra). In sintesi, l'ecosistema UAS+IA rende strutturale l'asimmetria tra operatori e interessati e fragile la praticabilità di modelli "consenso-centrici". La licenza sociale del trattamento – oltre che la sua liceità giuridica – passa per architetture di prevenzione²⁵: *privacy by design/default*, *data minimization*, *selective disclosure* e documentazione probatoria *ex ante* dell'adeguatezza delle misure. Questo impianto non è meramente difensivo: è il presupposto dogmatico della successiva costruzione della responsabilità civile, nella quale l'ordinamento europeo valorizza il nesso fra regole di prevenzione e regole di responsabilità e pone al centro l'idoneità preventiva delle misure come chiave di lettura della colpa e del nesso causale.

L'assetto regolatorio che incornicia l'uso dei droni e, soprattutto, ne condiziona la responsabilità per illecito trattamento dei dati ha una struttura a strati: a) la disciplina "aeronautica" europea e nazionale, improntata a un approccio *risk-based*; b) il diritto della protezione dei dati (GDPR e Codice Privacy) quale cornice orizzontale di liceità, trasparenza e sicurezza del trattamento; c) la regolazione contenuta nell'AI Act²⁶, che interviene sui profili riguardanti la qualità dei dati, la documentazione, la tracciabilità e la supervisione umana dei sistemi ad alto rischio²⁷, oggi spesso integrati negli UAS. È in

²⁴ Il reg. (UE) n. 1689/2024 sull'intelligenza artificiale ha modificato il reg. (UE) n. 1139/2018, imponendo il rispetto dei requisiti di cui al Capo III, Sez. 2, del regolamento sull'IA, allo scopo di garantire la conformità dei sistemi di IA impiegati nei droni a *standard* elevati di sicurezza e affidabilità, in linea con l'obiettivo dell'Unione di promuovere un'intelligenza artificiale che sia non solo innovativa, ma anche sicura (v., in tal senso, G. FINOCCHIARO, *La proposta di regolamento sull'intelligenza artificiale: il modello europeo basato sulla gestione del rischio*, in *Dir. inf.*, 2022, p. 303 ss.; C. SCHEPISI, *Brevi note sulla 'dimensione europea' della regolamentazione dell'intelligenza artificiale: principi, obiettivi e requisiti*, in V. FALCE (a cura di), *Strategia dei dati e intelligenza artificiale. Verso un nuovo ordine giuridico del mercato*, Torino, 2024, p. 53 ss.).

²⁵ Sul punto, si veda anche R. DUCATO, *Droni per il search and rescue in aree valanghine: profili privatistici*, in E. PALMERINI, M.A. BIASIOTTI e G.F. AIELLO (a cura di), *Diritto dei droni*, cit., p. 26.

²⁶ Esso fornisce un quadro normativo tecnologicamente neutro, modulato sul rischio, distinguendo i sistemi di IA in quattro categorie, basate appunto sul livello di rischio che presentano: inaccettabile, alto, specifico e limitato, e stabilendo, per ciascuna di queste, divieti, requisiti minimi obbligatori (alla cui stregua progettare e sviluppare i sistemi di IA), obblighi di trasparenza o semplici misure volte a promuovere l'autoregolamentazione. In dottrina, con riguardo all'approccio incentrato sulla *risk regulation*, cfr. G. SMORTO, *Distribuzione del rischio e tutela dei diritti nel Regolamento europeo sull'intelligenza artificiale. Una riflessione critica*, in *Foro it.*, 2024, V, c. 208 ss.; J. CHAMBERLAIN, *The Risk-Based Approach of the European Union's Proposed Artificial Intelligence Regulation: Some Comments from a Tort Law Perspective*, in *Eur. J. Risk Reg.*, 1/2023, p. 8 ss.

²⁷ A differenza dei sistemi di IA che determinano rischi inaccettabili, la qualificazione di un sistema di IA come «ad alto rischio», caratterizzato cioè dalla presenza di un pericolo significativo per la salute, la sicurezza

questo triangolo che si definisce il “grado” di diligenza esigibile dal titolare del trattamento e, correlativamente, il perimetro della sua esposizione al rimedio risarcitorio.

Il reg. (UE) n. 1139/2018 (*Basic Regulation*) ha superato la frammentazione precedente, assoggettando gli UAS a un quadro unitario e soprattutto a un modello di regolazione per rischio: categorie operative e requisiti tecnici non dipendono dalla finalità (ricreativa/professionale), bensì dal grado di rischio dell’operazione (proporzionalità e progressione)²⁸. Il regolamento qualifica come requisito essenziale per gli aeromobili senza equipaggio la considerazione, sin dalla progettazione e per impostazione predefinita, dei principi di tutela della riservatezza e della protezione dei dati, onde consentire l’identificazione dell’aeromobile e la comprensibilità della sua funzione. Tale impianto è stato completato dal reg. (UE) n. 945/2019 (aspetti di prodotto, classi, marcature, caratteristiche) e dal reg. (UE) n. 947/2019 (operazioni, categorie *open/specific/certified*, obblighi dell’operatore, *risk assessment*), i quali delineano una catena di responsabilità in cui le misure tecnico-organizzative di sicurezza e minimizzazione sono presupposto del volo stesso, non meri accorgimenti postumi.

A valle, l’ordinamento italiano ha completato il mosaico: il Regolamento ENAC UAS-IT del 4 gennaio 2021 richiama espressamente l’osservanza del GDPR e del Codice *Privacy*, enfatizzando il principio di minimizzazione e l’obbligo di menzionare il trattamento nella documentazione autorizzativa (art. 29). Con la circolare ATM-09A del 24 marzo 2021 sono state poi individuate nello spazio aereo italiano delle peculiari aree geografiche, classificandole come R («regolamentate»), P («proibite») e D («pericolose») in attuazione dell’art. 15 reg. es. (UE) n. 947/2019, nelle quali operazioni possono essere vietate o condizionate anche per ragioni di tutela della *privacy*: il che conferma l’intreccio, a livello operativo, fra *safety/security* e protezione dei dati.

Non irrilevante, infine, l’art. 56, § 8, *Basic Regulation*, che fa salva la facoltà degli Stati membri di stabilire regole nazionali per subordinare l’impiego degli UAS a condizioni poste – tra l’altro – «per la protezione della riservatezza e dei dati personali», purché nel rispetto del diritto dell’Unione. Tale clausola legittima interventi regolatori nazionali integrativi (come quelli richiamati da ENAC e dal Garante), i quali, se rispettosi dei principi

o i diritti fondamentali, non comporta un divieto, ma l’obbligo di ricondurre i rischi generati da questi sistemi entro livelli accettabili (v., tra gli altri, D. CHIAPPINI, *Intelligenza Artificiale e responsabilità civile: nuovi orizzonti di regolamentazione alla luce dell’Artificial Intelligence Act dell’Unione europea*, in *Riv. it. inf. dir.*, 2022, p. 102; S. ORLANDO, *Regole di immissione sul mercato e “pratiche di intelligenza artificiale” vietate nella proposta di “artificial intelligence act”*, in *Pers. merc.*, 2022, p. 346 ss.).

²⁸ Sull’applicazione del Regolamento, cfr. – tra gli altri – L. NAPOLITANO, *I droni ad uso civile nella prospettiva legislativa*, in R. BELLOTTI e L. TAFARO (a cura di), *Mezzi aerei a pilotaggio remoto: questioni teoriche e profili applicativi*, cit., p. 65 ss.; A. ZAMPONE, *L’impiego dei droni nelle operazioni in ambito civile, tra realtà operativa e prospettive di ulteriori opportunità. Una breve riflessione sull’attuale quadro normativo europeo*, in *Riv. mar.*, 2021, p. 46 ss.

UE, contribuiscono a concretizzare lo *standard* di diligenza dell'operatore anche agli effetti della responsabilità.

La disciplina “aeronautica” governa come si vola; il GDPR governa come si trattano i dati: quest'ultimo si applica a ogni trattamento di dati personali (art. 4, § 1) effettuato mediante UAS, fatta salva la stretta eccezione domestica (art. 2, § 2, lett. c), da interpretare restrittivamente, tanto che riprese «per fini personali» che incidano su spazi pubblici o vengano poi diffuse in rete escono agevolmente dall'ombrello della deroga²⁹. I principi di liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione; esattezza; limitazione della conservazione; integrità e riservatezza; e responsabilizzazione costituiscono il canone valutativo con cui saranno giudicate le scelte del titolare *ex ante* ed *ex post* (art. 5 GDPR)³⁰.

L'effetto sistemico è una convergenza: i requisiti di *safety* aeronautica e di affidabilità dell'IA fungono da *standard* di perizia anche per il giudizio sulla colpa del titolare/responsabile in caso di *data breach* o trattamento illecito. La funzione delle fonti sin qui richiamate non è meramente organizzativa; queste determinano la misura dell'aspettativa normativa: un operatore UAS che ometta la DPIA pur in presenza di sorveglianza sistematica su larga scala; che non dimostri la minimizzazione *ex ante*; che trascuri la cifratura, la gestione delle chiavi e la tracciatura dei *log*, in misura commisurata alla natura e al rischio dei flussi di dati personali (specie se appartenenti a categorie particolari *ex art.* 9 GDPR); che non attesti la supervisione umana del modulo IA ad alto rischio; o che ignori i vincoli geografici (zone P/D/R) posti anche a tutela della *privacy*, alimenta un giudizio di inadeguatezza delle misure sotto il profilo degli artt. 24 e 32 GDPR. In altre parole, il precetto di prevenzione si proietta sulla valutazione di colpa e sulla causalità dell'evento dannoso nel quadro dell'art. 82 GDPR, secondo un'impostazione che coordina regole di prevenzione e regole di responsabilità, respingendo letture *de minimis* del danno e valorizzando la dimostrazione dell'adeguatezza *ex ante* delle misure come prova liberatoria del titolare/responsabile.

In conclusione, il quadro integrato non si limita a “consentire” le operazioni UAS, ma fissa lo *standard* per giudicare la responsabilità in caso di illecito trattamento: progettare e

²⁹ Su tale costante orientamento giurisprudenziale, si vedano – *ex multis* – Corte giust., 6 novembre 2003, c.101/01, Bodil Lindqvist, in eur-lex.europa.eu, § 47, ove si afferma che l'esenzione per le attività a carattere domestico deve «interpretarsi nel senso che comprende unicamente le attività che rientrano nell'ambito della vita privata o familiare dei singoli, il che manifestamente non avviene nel caso del trattamento di dati personali consistente nella loro pubblicazione su Internet in modo da rendere tali dati accessibili ad un numero indefinito di persone», e Corte giust., 11 dicembre 2014, c. 212/13, František Ryneš, *ivi*, § 35, secondo cui il trattamento di dati personali mediante una telecamera di sorveglianza installata da una persona fisica sulla propria abitazione familiare non rientra nella deroga relativa alle attività esclusivamente personali o domestiche se la sorveglianza si estende anche a spazi pubblici.

³⁰ Sul punto, v. E. LUCCHINI GUASTALLA, *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in *Contr. impr.*, 2018, p. 111 ss.; D. POLETTI, *Le condizioni di liceità del trattamento dei dati personali*, in *Giur. it.*, 2019, p. 2783 ss.; F. BRAVO (a cura di), *Dati personali: protezione, libera circolazione e governance*, cit.

dimostrare misure adeguate non è un orpello regolatorio, bensì la condizione di liceità del volo-dato e la chiave di volta del giudizio di *liability*.

4. *Il modello di responsabilità per illecito trattamento ex art. 82 GDPR: accountability, colpa presunta e prova liberatoria.* La traiettoria del Regolamento (UE) 2016/679 è eminentemente prevenzionale: l'illecito trattamento non è un "rischio d'impresa" da contabilizzare a valle, ma un evento da prevenire a monte mediante scelte progettuali, organizzative e documentali verificabili. In questa prospettiva l'*accountability*³¹ opera come canone di diligenza professionale e, insieme, come architettura probatoria: il titolare deve poter dimostrare, *ex ante* ed *ex post*, la conformità del ciclo di vita del trattamento agli *standard* di legge, con particolare attenzione alle operazioni di captazione, trasmissione, annotazione e analisi tipiche degli UAS.

In sintesi, la prevenzione è il cuore della *data liability* in ambito UAS e IA: progettare per minimizzare³², impostare per difetto, valutare l'impatto, documentare ogni scelta e sottoporre ad *audit* la filiera tecnologica costituiscono non solo condizioni di liceità del trattamento, ma anche la migliore difesa – sul terreno della responsabilità – di fronte a pretese risarcitorie per illecito trattamento dei dati personali. L'ancoraggio normativo è l'art. 82 GDPR³³, il quale, da una parte, stabilisce che chiunque subisca un «danno materiale o immateriale»³⁴ causato da una violazione del regolamento ha il diritto di ottenere il

³¹ Cfr., ad esempio, G. FINOCCHIARO, *Il principio di accountability*, cit., p. 2778 ss., ove tra l'altro si mette in evidenza il duplice obbligo, «di conformarsi e di dimostrare», racchiuso nel principio; D. BARBIERATO, *Trattamento dei dati personali e «nuova» responsabilità civile*, in *Resp. civ. prev.*, 2019, p. 2153 s.; F. ALBANESE e I. CARDINALI, *Il principio di responsabilizzazione (accountability)*, in *Dati personali: protezione, libera circolazione e governance*, cit., p. 524 s.

³² I dati personali devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (cfr. S.G. BATTISTINI, L. MATARAZZO e L. ZANETTI, *Il principio di minimizzazione dei dati*, in *Dati personali: protezione, libera circolazione e governance*, cit., p. 231 ss.).

³³ Ne sottolineano, tuttavia, l'incompletezza, *ex multis*, F. BRAVO, *Riflessioni critiche sulla natura della responsabilità da trattamento illecito di dati personali*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, 2019, p. 383 ss.; F. BILOTTA, *La responsabilità civile nel trattamento dei dati personali*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice privacy)*, Milano, 2019, p. 391.

³⁴ Tale espressione è, in realtà, il frutto di una non felice trasposizione di termini giuridici (danno patrimoniale e non patrimoniale). Tuttavia, essa esprime con chiarezza l'intenzione che la ispira: garantire al danneggiato un pieno ed effettivo risarcimento per il pregiudizio derivante dall'illecito trattamento di dati personali, come impone l'inerenza di tale attività ai diritti e alle libertà fondamentali della persona [cfr., al riguardo, le osservazioni di P. PERLINGIERI, *La responsabilità civile tra indennizzo e risarcimento*, in *Rass. dir. civ.*, 2004, p. 1061 ss., il quale esorta a spostare l'attenzione «dalla patrimonialità o non patrimonialità del danno per riportarla più correttamente sulla patrimonialità o non patrimonialità dell'interesse leso, in ossequio agli originali intenti perseguiti ed esplicitati attraverso l'elezione del risarcimento quale reazione, tra le diverse attuabili, alla lesione di un interesse protetto»: peraltro, il punto centrale della responsabilità oggi è «non tanto l'*an* (l'individuazione della meritevolezza dell'interesse – là dove ormai alcuni interessi di rilevanza costituzionale non possono

risarcimento del danno dal titolare o dal responsabile del trattamento (§§ 1 e 2), e dall'altra, che questi ultimi sono esonerati dalla responsabilità se dimostrano che l'evento dannoso non gli è in alcun modo imputabile (§ 3). L'architettura normativa si traduce in un meccanismo di responsabilità per colpa con inversione dell'onere della prova³⁵: non grava sul danneggiato provare il dolo o la negligenza; grava, viceversa, su titolare e responsabile provare l'adeguatezza *ex ante* delle misure tecnico-organizzative e, quindi, l'assenza di colpa rispetto alla violazione che ha causato il pregiudizio. In tal senso, il diritto alla protezione dei dati non è soltanto matrice di regole di prevenzione, ma anche parametro per giudicare la diligenza dell'operatore, alla luce dei principi di responsabilizzazione e gestione del rischio che innervano l'intero sistema.

Sotto il vigore dell'art. 15 d.lgs. n. 196/2003 – che rinviava all'art. 2050 c.c. – la responsabilità civile per illecito trattamento era letta, in larga parte, come responsabilità oggettiva (o comunque aggravata)³⁶, con onere liberatorio a carico del danneggiante di provare l'adozione di tutte le misure idonee a evitare il danno³⁷. L'abrogazione di quella

essere tenuti fuori dalla tutela anche risarcitoria –), ma il *quantum damni* in una prospettiva di solidarietà sostenibile, attenta al bilanciamento dei principi e valori coinvolti»].

³⁵ In tale prospettiva, la responsabilità da trattamento dei dati personali diviene paradigmatica di una tendenza a collegare la responsabilità extracontrattuale a comportamenti che un soggetto avrebbe potuto e/o dovuto assumere, nella consapevolezza degli obblighi e dei rischi che vi sono tipologicamente connessi.

³⁶ Cfr., per tutti, M. FRANZONI, *Responsabilità per l'esercizio di attività pericolose*, in G. ALPA e M. BESSONE (a cura di), *La responsabilità civile*, II, 2, Torino, 1987, p. 459.

³⁷ G. COMANDÉ, sub art. 15 D.lgs. n. 196/2003, in C.M. BIANCA e F.D. BUSNELLI (a cura di), *La protezione dei dati personali. Commentario al D. Lgs. 30 giugno 2003, n. 196 «Codice della privacy»*, Padova, 2007, p. 393, sostiene che la prova di aver adottato «tutte le misure idonee ad evitare il danno» debba leggersi come prova critica dell'esistenza di un fattore idoneo a rendere «impossibile l'adempimento del dovere legale».

L'art. 15, comma 2, stabiliva anche la risarcibilità del danno non patrimoniale in caso di violazione dell'art. 11, riguardante le modalità del trattamento e i requisiti dei dati, rimettendo all'interessato la dimostrazione dell'esistenza del danno, di una condotta contraria alla normativa a tutela dei dati personali e della relazione causale tra i primi due elementi. Tuttavia, a determinare una lesione ingiustificabile del diritto non sarebbe la mera inosservanza delle prescrizioni poste dall'art. 11, ma solo quella che ne offenda in modo sensibile la portata effettiva: cfr. Cass., 15 luglio 2014, n. 16133, in *Danno resp.*, 2015, p. 339 ss., con note di V. CECCARELLI, *La soglia di risarcibilità del danno non patrimoniale da illecito trattamento dei dati personali*, e M. NITTI, *La valutazione della "gravità della lesione" e della "serietà del danno" nel risarcimento del danno non patrimoniale da violazione della privacy*, ove si sottolinea che il danno non patrimoniale, pur determinato da una lesione del diritto fondamentale alla protezione dei dati personali tutelato dagli artt. 2 e 21 cost. e dall'art. 8 CEDU, non si sottrae alla verifica della «gravità della lesione» e della «serietà del danno» (quale perdita di natura personale effettivamente patita dall'interessato), poiché anche per tale diritto opera il bilanciamento con il principio di solidarietà *ex art. 2 cost.*, di cui il principio di tolleranza della lesione minima è intrinseco precipitato; Cass., 5 marzo 2015, n. 4443, in *giustiziacivile.com*, 7/2015, con nota di S. ALBERTI, *Illecito trattamento dei dati personali: il danno non patrimoniale non è in re ipsa*; Cass., 15 ottobre 2015, n. 20890, *ivi*, 2016, p. 372 ss., con nota di M. GAGLIARDI, *La prova del danno non patrimoniale in caso di trattamento illecito di dati personali*; Cass., 23 maggio 2016, n. 10638, in *CED online*, 2016; Cass., 3 agosto 2017, n. 19423, in *Dir. giust.*, 2017; Cass., 12 maggio 2023, n.

norma e l'entrata in vigore del GDPR hanno riaperto il dibattito sul criterio di imputazione: parte della dottrina ha insistito sulla responsabilità oggettiva³⁸, altri hanno ricondotto l'illecito a una presunzione di colpa³⁹, altri ancora hanno sperimentato costruzioni *ex art.* 1218 c.c. o modelli misti calibrati sul grado di rischio del trattamento⁴⁰.

La Corte di Giustizia, da par sua, ha accolto la tesi che ricostruisce l'imputazione della responsabilità, al titolare o al responsabile del trattamento, come fondata su un «meccanismo di responsabilità per colpa accompagnato da un'inversione dell'onere della prova»⁴¹: non grava, quindi, sul danneggiato l'onere di provare il dolo o la negligenza nell'attività di trattamento, giacché tali profili soggettivi sono presunti sino a prova contraria, per la semplice circostanza che si è verificato un trattamento violativo del

13073, in *Nuove leggi civ. comm.*, 2023, I, p. 1133 ss., con commento di G.M. RICCIO, *Dati personali e rimedi: diritti degli interessati e profili risarcitori*.

³⁸ In termini oggettivi, pur nella varietà di accenti, si vedano S. SICA, sub *art. 82 GDPR*, in *Codice della privacy e data protection*, a cura di R. D'Orazio, G. Finocchiaro, O. Pollicino e G. Resta, Milano, 2021, p. 893, secondo cui la prova liberatoria consisterebbe non nella «nella mera allegazione della massima diligenza esigibile ma nella dimostrazione di un fatto terzo generatore del danno, munito dei caratteri di imprevedibilità ed inevitabilità proprio del caso fortuito e della forza maggiore»; A. MAIETTA, *La prova del danno da illecito trattamento dei dati personali*, Roma, 2023, p. 86 ss.; E. TOSI, *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, Milano, 2019, p. 125, che si è espresso in termini di responsabilità oggettiva per rischio d'impresa, derivante da un'attività di trattamento dei dati personali posta in essere in dispregio delle regole di condotta protettive del danneggiato/interessato, soggetto debole del rapporto asimmetrico che il trattamento dei dati genera.

³⁹ Per una lettura in termini di colpa presunta, senza alcuna pretesa di esaustività, cfr. M. GAMBINI, *Principio di responsabilità e tutela aquiliana dei dati personali*, Napoli, 2018, p. 68 ss.; C.M. BIANCA, *Diritto civile*, 5, *La responsabilità*, Milano, 1995, p. 709; M. FRANZONI, *Dati personali e responsabilità civile*, in *Resp. civ. prev.*, 1998, p. 902, il quale dubita che si possa ragionevolmente equiparare il trattamento dei dati personali e la produzione di polveri da sparo o di bombole del gas o l'attività di un imprenditore chimico; U. RUFFOLO, *Dati personali: trattamento e responsabilità*, in V. CUFFARO, V. RICCIUTO e V. ZENO ZENCOVICH (a cura di), *Trattamento dei dati e tutela della persona*, Milano, 1998, p. 281 ss.; F.D. BUSNELLI, *Il «trattamento dei dati personali» nella vicenda dei diritti della persona: la tutela risarcitoria*, *ivi*, p. 183; E. PELLECCIA, *La responsabilità civile per trattamento dei dati personali*, in *Resp. civ. prev.*, 2006, p. 221 ss.; F. MACARIO, *La protezione dei dati personali nel diritto privato europeo*, in V. CUFFARO e V. RICCIUTO (a cura di), *Il trattamento dei dati personali*, Torino, 1997, p. 48 ss., note 104 e 108; G. NAVONE, *Ieri, oggi e domani della responsabilità civile da illecito trattamento dei dati personali*, in *Nuova leggi civ. comm.*, 2022, p. 132.

⁴⁰ Si vedano, seppur con diversità di accenti, F. BILOTTA, *La responsabilità civile nel trattamento dei dati personali*, cit., p. 453; F. BRAVO, *Riflessioni critiche sulla natura della responsabilità da trattamento illecito di dati personali*, cit., p. 384 ss.; U. SALANITRO, *Illecito trattamento dei dati personali e risarcimento del danno nel prisma della corte di giustizia*, in *Riv. dir. civ.*, 2023, p. 450 s.

⁴¹ Cfr., in particolare, Corte giust., 21 dicembre 2023, c. 667/21, ZQ c. Medizinischer Dienst der Krankenversicherung Nordrhein, Koöperschaft des öffentlichen Rechts, in [curia.europa.eu](https://eur-lex.europa.eu/curia/europa.eu), spec. § 98. Del medesimo avviso, in sostanza, sia la di poco precedente Corte giust., 14 dicembre 2023, c. 340/21, VB c. Natsionalna agentsia za prihodite, in *Danno resp.*, 2024, p. 567 ss., con commento di C. BRIGNOLO, *Violazione dei dati personali: responsabilità e danni risarcibili*, che le successive Corte giust., 25 gennaio 2024, c. 687/21, BL c. MediaMarktSaturn Hagen-Iserlohn GmbH, in [curia.europa.eu](https://eur-lex.europa.eu/curia/europa.eu), spec. § 35 ss., e Corte giust., 11 aprile 2024, c. 741/21, GP c. Juris GmbH, *ivi*, §§ 44-54.

GDPR. Dagli arresti della Corte risulta, in maniera netta, il tentativo di conciliare, o meglio coordinare, regole di prevenzione e regole di responsabilità: infatti, se alla luce degli artt. 24 e 32 GDPR, sul titolare del trattamento incombe il dovere di adottare misure tecniche e organizzative destinate ad evitare, per quanto possibile, qualsiasi violazione di dati personali; dall'altra, l'adeguatezza di siffatte misure "preventive" deve essere valutata «in concreto», esaminando se queste siano state attuate dal titolare del trattamento in maniera proporzionata alla relativa probabilità e gravità, da apprezzare in relazione alla natura, al contesto, all'ambito applicativo e alla finalità del trattamento stesso⁴². In altri termini, la dimostrazione, da parte del soggetto attivo del trattamento, «che non sussiste alcun nesso di causalità tra la sua eventuale violazione dell'obbligo di protezione dei dati e il danno subito dalla persona fisica»⁴³ finisce col tradursi nella capacità di comprovare l'adeguatezza *ex ante* delle misure rispetto al rischio.

Nel contesto UAS, tale approccio dialoga direttamente con gli *standard* aeronautici *risk-based* (reg. UE n. 1139/2018; reg. UE n. 945/2019; reg. UE n. 947/2019) e con gli obblighi ENAC UAS-IT, i quali concorrono a determinare lo standard di diligenza esigibile dall'operatore anche ai fini dell'illecito *privacy*. Il danneggiato deve fornire la prova: *a*) di una violazione del GDPR (ad esempio, mancanza di base giuridica; DPIA omessa, ove necessaria; misure di sicurezza insufficienti; carenze informative; trattamenti eccedenti i principi di minimizzazione o limitazione della finalità; uso di biometria senza base *ex art.* 9); *b*) di un danno (materiale o immateriale); *c*) dell'anello causale tra violazione e danno. Non deve dimostrare la colpa in senso stretto, che è presunta. Incombe invece su titolare e responsabile la prova liberatoria: dimostrare puntualmente che la violazione non è loro imputabile in colpa, perché le misure adottate erano adeguate al rischio (*accountability ex ante*, art. 24; sicurezza *ex art.* 32; protezione *by design/default ex art.* 25; DPIA *ex art.* 35).

Nel GDPR la causalità è normativamente orientata dalle regole di prevenzione. Gli artt. 24, 25 e 32 impongono misure proporzionate alla probabilità e gravità del pregiudizio: la loro inadeguatezza – specie se attinente a minimizzazione, sicurezza o DPIA in scenari

⁴² Ciò risulta perfettamente in linea con un'interpretazione sistematica del riferito quadro normativo, anche alla luce dei considerando da 4 a 8 GDPR, dai quali emerge che obiettivo del Regolamento è proprio la ricerca di un "bilanciamento" tra gli interessi dei titolari del trattamento di dati personali e i diritti delle persone cui lo stesso trattamento si riferisce: consentire lo sviluppo dell'economia digitale, garantendo, nel contempo, un elevato livello di tutela delle persone fisiche. Tale "equilibrio" appare maggiormente assicurato da un meccanismo di responsabilità per colpa accompagnato da un'inversione dell'onere della prova: non sarebbe conforme all'obiettivo di una protezione elevata optare per un'interpretazione in base alla quale gli interessati che abbiano subito un danno a causa di una violazione del GDPR debbano, nell'ambito di un'azione di risarcimento *ex art.* 82, farsi carico dell'onere di provare non solo l'esistenza di tale violazione e del danno che ne è disceso, ma anche l'esistenza di una colpa del titolare del trattamento o addirittura il grado di tale colpa; dall'altro, neppure un regime di responsabilità oggettiva garantirebbe la realizzazione dell'obiettivo di certezza giuridica per operatori economici, autorità pubbliche e interessati, come risulta dal considerando 7 GDPR, sul presupposto che l'attribuzione di una responsabilità a dispetto dell'adeguatezza delle misure metterebbe la stessa sempre in discussione, svuotandola di significato.

⁴³ Secondo il periodare di Corte giust., 14 dicembre 2023, c. 340/21, cit., § 72.

UAS di sorveglianza sistematica su larga scala – funge da indice qualificato della colpa e, spesso, da ponte logico verso la causalità dell’evento. Al contrario, una progettazione robusta e documentata offre elementi per rompere la catena causale o attenuarne la portata.

Peraltro, la giurisprudenza europea⁴⁴ ha escluso: *a*) che la mera violazione basti da sola a fondare il risarcimento; *b*) che si possano introdurre soglie di gravità (*de minimis*) non previste dalla norma⁴⁵; *c*) il danno *in re ipsa*, richiedendo la prova delle conseguenze negative. In altri termini: niente soglie di gravità, ma onere di allegazione/prova delle ripercussioni concrete; niente automatismi, ma rigore probatorio. Tale equilibrio tutela insieme i diritti degli interessati e la libera circolazione dei dati, impedendo derive punitivo-dissuasive non contemplate dal regolamento.

Tuttavia, la soluzione che esclude il risarcimento, se non s’è data una prova circostanziata e precisa del danno, risulta troppo drastica, occorrendo invece distinguere in base alla natura dell’interesse protetto: un conto è il danno alla persona, altro conto il danno a cose o a rapporti economici⁴⁶. Proprio la diffusione non autorizzata e non conforme alla legge di dati personali o la violazione della *privacy* generano danni apprezzabili *ex se* meritevoli di risarcimento⁴⁷.

⁴⁴ Si veda quanto affermato da Corte giust., 14 dicembre 2023, c. 456/22, VX, AT c. Gemeinde Ummendorf, in [curia.europa.eu](https://eur-lex.europa.eu/juris/ces/?uri=CELEX:20231214_0456_22_VX_AT_C_Gemeinde_Ummendorf); Corte giust., 14 dicembre 2023, c. 340/21, cit.; Corte giust., 25 gennaio 2024, c. 687/21, cit.; Corte giust., 11 aprile 2024, c. 741/21, cit.; Corte giust., 20 giugno 2024, c. 590/22, T e BT. c. PS GbR, VG, MB, DH, WB e GS, in [curia.europa.eu](https://eur-lex.europa.eu/juris/ces/?uri=CELEX:20240620_0590_22_T_BT_C_PS_GbR_VG_MB_DH_WB_GS).

⁴⁵ Diversamente, la giurisprudenza italiana non ha mai inteso discostarsi dall’insegnamento delle c.dd. sentenze di San Martino delle Sezioni Unite (Cass. civ., Sez. un., 11 novembre 2008, nn. 26972-26975, in *Danno resp.*, 2009, p. 19 ss.) sull’irrisarcibilità dei pregiudizi bagatellari, giacché «la lesione deve eccedere una certa soglia di offensività, rendendo il pregiudizio tanto serio da essere meritevole di tutela in un sistema che impone un grado minimo di tolleranza», in forza del principio di solidarietà sociale sancito dall’art. 2 Cost. Tale orientamento è stato però condivisibilmente criticato dalla dottrina (v., anche per gli ampi riferimenti bibliografici, F. BRAVO, *Il principio di solidarietà in materia di protezione dei dati personali nelle decisioni del Garante e della Corte di Cassazione*, in *Contr. impr.*, 2023, pp. 405 ss. e 426 ss.), specie perché, così opinando, si giunge a riservare ai diritti inviolabili della persona (entro una certa soglia – imposta – di tolleranza) un trattamento risarcitorio deteriore rispetto al patrimonio, così sovvertendo la gerarchia assiologica della Costituzione.

⁴⁶ Di tale opinione anche G. ALPA, *Danno in re ipsa e tutela dei diritti fondamentali (diritti della personalità e diritto di proprietà)*, in *Resp. civ. prev.*, 2023, p. 11, e C. CAMARDI, *Illecito trattamento dei dati e danno non patrimoniale. Verso una dogmatica europea*, in *Nuove leggi civ. comm.*, 2023, II, p. 1143, secondo cui «una volta realizzatasi la lesione del diritto della persona attraverso la violazione della regola di condotta che lo protegge da interferenze ed offese altrui, ciò [dovrebbe essere] sufficiente a determinare contestualmente l’insorgenza di un danno non patrimoniale risarcibile, senza che l’interessato debba fornire ulteriori prove, ed in ragione della natura tutta speciale del diritto leso e del danno di cui si chiede ristoro: l’uno, diritto della persona non patrimonializzabile; l’altro, per sua natura liquidabile già in relazione alla gravità dell’illecito, e non ad una perdita emergente o a un mancato guadagno. Ciò che di solito si riassume nell’espressione per la quale in tali casi il danno non patrimoniale sarebbe *in re ipsa*».

⁴⁷ «La condotta illecita che produce lesione del diritto della persona è danno evento e al tempo stesso danno conseguenza, perché la “natura” del diritto leso, il valore personale non patrimoniale, postula che l’ordinamento debba garantire la sua integrità a fronte di condotte illecite interferenti, e non – come per gli

In relazione, invece, al *quantum* del risarcimento pecuniario fondato sull'art. 82 GDPR, esso può essere considerato «pieno ed effettivo»⁴⁸ se consente di compensare integralmente il danno concretamente subito a causa della violazione del regolamento, che non contempla anche una funzione dissuasiva o punitiva, impedendo che il livello dell'importo risarcitorio possa andare oltre la piena compensazione⁴⁹.

5. *Persona e proporzionalità nella legittimità del volo-dato*. In conclusione, l'art. 82 GDPR – letto alla luce della responsabilizzazione e della prevenzione – consegna uno statuto europeo della responsabilità civile per illecito trattamento che, nel dominio UAS+IA, premia chi progetta e dimostra: colpa presunta ma vincibile mediante prova di adeguatezza *ex ante*; nesso causale orientato dalle regole di prevenzione e dalla qualità dell'assetto organizzativo; danno senza soglie, ma senza automatismi né danno *in re ipsa* e con funzione meramente compensativa.

Su questa linea di crinale, tra innovazione e tutela, si misura la maturità degli operatori e l'effettività dei diritti: l'innovazione – anche quando “vola” – non è un fine, ma un mezzo che deve piegarsi alla primazia della persona e alla proporzionalità dell'interferenza⁵⁰.

L'esperienza dei droni, ormai uscita da tempo dall'alveo militare, mostra con chiarezza l'ambivalenza dei nuovi ecosistemi dati: straordinarie opportunità (ambiente, sicurezza, logistica) si accompagnano a rischi inediti per la sfera privata, acuiti dalla capacità di

altri diritti individuali patrimoniali – a fronte di perdite patrimoniali; le quali peraltro nemmeno sono concepibili rispetto ad un valore primario e inviolabile: salvo che si voglia negare la distinzione tra persona e mercato» (C. CAMARDI, *op. cit.*, p. 1144).

⁴⁸ Corte giust., 4 maggio 2023, c. 300/2021, UI c. Österreichische Post AG, § 58, in *Foro it.*, 2023, IV, c. 268 ss., con note di A. PALMIERI e R. PARDOLESI, *Mai futile il danno non patrimoniale da violazione della privacy (purché lo si provi!)*; S. PAGLIANTINI, *Un altro palcoscenico della “guerra” tra le corti: il danno (immateriale) bagatellare dell'art. 82 Gdpr*; M. FEDERICO, *“La tempesta perfetta”: ultime dalla Corte di Lussemburgo su danno (non patrimoniale) da illecito trattamento dei dati personali e possibili risvolti in tema di tutela collettiva*; e in *Nuove leggi civ. comm.*, 2023, I, p. 1119 ss., con commento di G. CALABRESE, *Il danno da “perdita di controllo dei dati personali” nel pensiero della Corte di Giustizia UE*.

⁴⁹ Cfr. Corte giust., 21 dicembre 2023, c. 667/21, cit., § 98. *Contra*, in un'ottica di maggiore effettività della tutela, v. E. TOSI, *Responsabilità civile per illecito trattamento dei dati personali*, cit., spec. pp. 199 ss. e 268 ss.; ID., *Circolazione dei dati personali tra contratto e responsabilità. Riflessioni sulla fragilità del consenso e sulla patrimonializzazione dei dati personali nella società della sorveglianza digitale*, Milano, 2023, p. 152 ss.

⁵⁰ Sul principio di proporzionalità, v. P. PERLINGIERI, *Il diritto civile nella legalità costituzionale secondo il sistema italo-comunitario delle fonti*, 3^a ed., Napoli, 2006, p. 379 ss., per il quale tale principio opera tra elementi di raffronto omogenei e ha valenza sul piano quantitativo; diversamente, quando il collegamento è tra elementi disomogenei, non comparabili, che coinvolgono interessi non quantificabili, ad esempio, non patrimoniali, ne consegue un bilanciamento tra questi che esige necessariamente una valutazione qualitativa. In tali ipotesi, entrano in funzione sia il principio della ragionevolezza sia il principio dell'adeguatezza, utilizzati spesso in combinazione con il principio di proporzionalità. Inoltre, per una ricostruzione della tecnica del bilanciamento secondo ragionevolezza, v. G. PERLINGIERI, *Profili applicativi della ragionevolezza nel diritto civile*, Napoli, 2015, p. 102 ss.

raccolta massiva, dalla natura sovranazionale e delocalizzata dei flussi, dalla produzione di pregiudizi “diffusi” su platee ampie e mutevoli e dall’opacità dei modelli *self-learning*.

In questo contesto, il GDPR continua a dettare il canone, ma talune sue categorie – nate per relazioni più lineari tra interessato e titolare – sono messe alla prova dalle logiche dei *big data*; l’*AI Act*, per parte sua, rafforza l’assetto di affidabilità lungo il ciclo di vita dei sistemi, intervenendo sulla qualità dei dati, sulla documentazione, sulla tracciabilità e sulla supervisione umana (in particolare per i sistemi ad alto rischio). Ne discende una bussola metodologica unitaria fondata su: ragionevolezza e proporzionalità come criteri di governo del rischio; *accountability* quale architettura probatoria; prognosi postuma sull’adeguatezza delle misure come metrica della colpa. Sul piano operativo, *privacy by design* e *by default*, valutazione d’impatto (DPIA), minimizzazione, sicurezza lungo l’intero ciclo di vita del dato, trasparenza multilivello, assoggettabilità ad *audit* dell’intera filiera e controllo umano effettivo costituiscono presidi che assumono rilievo in giudizio.

Solo assumendo la persona quale stella polare – e coordinando in modo coerente regole aeronautiche *risk-based*, protezione dei dati e affidabilità dell’IA – il diritto potrà accompagnare la tecnologia senza cedere né al freno indiscriminato né alla deriva permissiva: è qui che si costruisce, caso per caso ed *ex ante* prima ancora che *ex post*, la legittimità del volo-dato e la credibilità della nostra *data liability*.